n.º 6, 2026

Revista Académica
de Tendências em
Comunicação
e Ciências
Empresariais

When technology is not enough: the role of internal communication in cybersecurity

Dulce Pereira

2090944@iscap.ipp.pt
https://orcid.org/0009-0001-1425-1199
ISCAP, Instituto Politécnico do Porto

Abstract

Organisations continue to strengthen their cybersecurity through technological investment, yet many security incidents still arise from routine employee practices. This article examines that limitation and argues that technology alone does not secure organisational environments. A more effective response depends on the interaction between internal communication, organisational culture, and employee behaviour. This interaction is reflected in internal communication that shapes how security requirements are interpreted and enacted in daily work, a shared culture that normalises protective conduct, and employee involvement in the enactment of secure behaviour. Drawing on literature on cybersecurity, organisational culture, and internal communication, the article frames digital protection as a socio-technical issue rather than a purely technical one. The discussion shows that risk often emerges when formal rules fail to connect with everyday routines. For that reason, cybersecurity should be managed as an organisational process in which technical measures, communication practices, and behavioural alignment are treated as mutually dependent.

Keywords: Cybersecurity, Culture, Internal Communication, Employee Behaviour

Resumo

Muitas organizações reforçam a cibersegurança através de investimento tecnológico, mas continuam a enfrentar falhas ligadas ao comportamento quotidiano dos colaboradores. Este artigo argumenta que a tecnologia, embora indispensável, não basta para garantir proteção eficaz. A segurança depende também da forma como a comunicação interna, a cultura organizacional e o comportamento dos colaboradores se articulam na prática. A análise mostra que grande parte da vulnerabilidade surge no desfasamento entre políticas formais e práticas reais de trabalho. Assim, a cibersegurança deve ser gerida como um processo organizacional integrado, e não apenas como uma resposta técnica.

Palavras-chave: Cibersegurança, Cultura, Comunicação Interna, Comportamento dos Colaboradores

Introduction

The increasing digitalisation of organisational activities has changed how information is created, accessed, and protected in today's workplaces. As organisations rely more on connected systems, cybersecurity is no longer limited to technical infrastructures, and is increasingly determined by employee behaviour, organisational culture, and internal communication.

Despite considerable investments in technological safeguards, security incidents remain frequent, often associated with employees' non-compliance with information security policies and risky behavioural practices (Bulgurcu et al., 2010; Pollini et al., 2022). This highlights the limitations of technology-centred approaches, as many cybersecurity failures are linked to organisational and behavioural factors.

While previous research has focused on individual aspects such as awareness, perceived risk, and behavioural intentions (Shahbaznezhad et al., 2021), these do not fully explain how security behaviour develops in different organisational contexts. Organisational culture, shared norms and expectations influence how employees interpret and respond to security requirements, reflecting the broader role of organisational information security culture in shaping behaviour (Alhogail, 2015; Da Veiga et al., 2020).

Nevertheless, these expectations do not always translate into practice. In organisational settings, internal communication plays an important role in clarifying security expectations and supporting how they are understood and applied in everyday work. It goes beyond sharing information, since it influences how employees understand their responsibilities, engage with security practices, and act in line with organisational objectives (Barlow et al., 2018; Rice & Searle, 2022).

By turning formal policies into practical guidance and reducing ambiguity in everyday decisions, communication supports more consistent security behaviour. As digital workplaces become more complex, effective cybersecurity depends on moving beyond isolated technological solutions and adopting integrated approaches which combine technical controls, communication, and active employee involvement (Saeed, 2023).

This article argues that organisational cybersecurity needs an integrated approach that brings together internal communication, organisational culture, and employee behaviour. These elements shape how security expectations are understood and applied in everyday work. Therefore, cybersecurity efficiency depends on communication practices that support consistent behaviour and lower human-related risks in organisational settings.

Human Factor and Information Security Behaviour

Employees play a central role in organisational cybersecurity because they continuously make and apply security-related decisions in their everyday work. Cybersecurity incidents do not emerge exclusively from technological failures, but often from the gap between formal security requirements and the realities of organisational practice. From this perspective, information security behaviour is shaped not only by technical controls or policy enforcement, but also by how employees interpret, negotiate, and apply security expectations within specific organisational contexts (Pollini et al., 2022).

This perspective challenges the widespread assumption that employees are simply the "weakest link" in cybersecurity. Rather than passive sources of risk, employees navigate competing demands, operational pressures, and time constraints that shape security-related decisions in practice. Consequently, behavioural vulnerabilities frequently emerge in social engineering and phishing scenarios, where routine actions and contextual judgement directly influence organisational exposure to risk (Aschwanden et al., 2024). The 2022 cyberattack on

Vodafone Portugal illustrates this dynamic particularly well. According to Vodafone's own reporting, the attack relied on "sophisticated social engineering" and a detailed understanding of internal systems and organisational processes (Vodafone, 2023). The incident disrupted mobile communications, emergency services, and critical organisational operations nationwide, reinforcing how cybersecurity incidents may emerge from the interaction between human behaviour, organisational routines, and technological infrastructures.

Empirical research further suggests that employee behaviour is influenced not only by awareness, but also by cognitive and contextual mechanisms that shape how security decisions are made in practice. Shahbaznezhad et al. (2021) argue that perceived threat influences behavioural intention, with its effects shaped by how individuals interpret both the likelihood and potential consequences of security incidents.

At the same time, routine-based behaviour reduces the role of conscious decision-making, as repeated task execution encourages employees to rely on automated actions that may bypass formal security procedures. Employees may, for example, click on familiar email links or reuse previously created passwords without actively evaluating potential risks, particularly when performing routine tasks. Similar dynamics may also emerge in physical security situations, such as allowing unfamiliar individuals to enter restricted areas out of courtesy or leaving devices unattended in shared workspaces. Situational pressures such as time constraints, task urgency, and performance demands may also reduce compliance, as employees frequently prioritise operational efficiency over security requirements. In these situations, employees may choose to share files through unsecured channels or bypass authentication procedures in order to meet immediate deadlines.

These dynamics suggest that awareness-based approaches alone are often insufficient, as they tend to assume rational and deliberate decision-making. In practice, however, security behaviour is frequently shaped by habits, routines, and situational pressures embedded within everyday organisational work.

Organisational Context and Security Behaviour

Within organisational contexts, policy compliance cannot be fully explained through knowledge or rational intention alone. Employees frequently make pragmatic trade-offs between security requirements and task efficiency, particularly under time pressure, competing priorities, or unclear procedural guidance. This suggests that compliance is shaped by how security measures are perceived in relation to everyday work demands (Bulgurcu et al., 2010). As such, security behaviour is not fixed or purely individual,but develops within organisational contexts in which formal expectations often clash with operational realities.

Consequently, organisational responses that rely exclusively on awareness programmes or technical controls tend to produce limited and inconsistent results. Behavioural change depends on how organisations combine training, communication and practical actions within everyday work practices (Alshaikh, 2020). Approaches such as continuous awareness initiatives, role-based engagement strategies, and integrated communication practices illustrate how organisations can move beyond compliance-driven models towards actively shaping employee behaviour.

When communication is unclear, generic, or not aligned with day-to-day activities, security policies tend to be perceived as abstract and disconnected from practice, leading to inconsistent behaviour. In these situations, employees often rely on informal exchanges or past experience to guide their actions, which may not always align with formal security expectations. Internal communication therefore plays a critical role in reducing ambiguity, supporting decision-making, and translating formal policies into actionable practices.

In practical terms, this requires communication to be embedded within workflows and supported by clear, usable procedures. Simplifying security requirements and aligning them with operational realities can reduce the need for workarounds, while timely and contextual guidance supports employees at the moment decisions are made. In addition, fostering a supportive security climate, where expectations are clear and incident reporting is not associated with blame, can strengthen engagement with secure behaviours.

Overall, the human factor should not be understood as an isolated source of vulnerability, but as a dynamic organisational process shaped by the interaction between individual behaviour, organisational conditions, and communication practices. Security behaviour emerges from the continuous interaction between formal rules and everyday work practices, highlighting the need for integrated organisational, behavioural and communication approaches.

Internal Communication and Cybersecurity Behaviour

Internal communication refers to the formal and informal processes through which information, expectations, and meanings are shared within an organisation (Tkalac Verčič et al., 2023). It includes structured channels, such as policies, training, and digital platforms, as well as routine interactions between employees. Beyond information sharing, it shapes how organisational priorities are interpreted and enacted in practice.

In the context of cybersecurity, this role becomes particularly relevant as it translates security expectations into everyday practices. It helps employees understand what is expected, how to act, and why it matters, connecting formal policies with everyday behaviour and aligning technology, organisational structures and employee actions (Barlow et al., 2018).

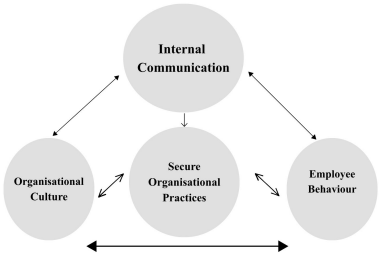
In practice, communication operates through both formal and informal channels. While organisations rely on structured mechanisms such as training and awareness campaigns, employees often turn to informal exchanges when guidance is unclear or not easily accessible. These interactions may shape behaviour more directly than formal rules, particularly in day-to-day decisions.

This becomes clearer when examining how employees interpret different types of messages. Communication determines not only what employees know, but how they prioritise security in practice. Barlow et al. (2018) distinguish between informational and normative communication. Informational communication explains rules, such as how to create strong passwords or recognise phishing emails, improving understanding but not always leading to behavioural change.

Normative communication operates differently by signalling what is expected within the organisation. Messages that reinforce shared responsibility for security, or highlight behaviours such as reporting suspicious activity, make expectations visible and socially reinforced, creating pressure to conform. Communication therefore operates at two levels: it supports understanding and defines what is considered appropriate behaviour. Both are necessary, as clarity enables action, while reinforcement sustains it.

Taken together, these dimensions suggest that secure organisational practices emerge from the interaction between communication processes, organisational culture, and employee behaviour rather than from technological controls alone.

Figure 1. Conceptual model of organisational cybersecurity practices.



Note.Source: Author's own elaboration based on reviewed literature.

Leadership, Communication and Organisational Context

The role of internal communication becomes particularly important when considering leadership and organisational culture, as it is the main mechanism through which leadership priorities are expressed. Hu et al. (2012) show that employee compliance is strongly influenced by top management support, largely conveyed through internal channels. When leadership consistently emphasises security, employees are more likely to prioritise it in their daily work. Men and Stacks (2014) further show that authentic leadership strengthens communication quality and builds trust.

In practice, this alignment is not always consistent across teams. When managers prioritise speed or task completion over compliance, employees may interpret security procedures as secondary, regardless of formal policies. These local signals often shape behaviour more directly than official guidelines. In this sense, leadership communication extends beyond formal messaging, as employees often interpret managerial behaviour itself as an indicator of organisational priorities. When leaders bypass procedures or implicitly reward speed over compliance, security requirements may gradually lose legitimacy within everyday work practices.

Internal communication also influences how employees perceive the organisational security environment. Goo et al. (2014) show that information security climate is reinforced through communication that signals expectations, support, and accountability. When communication is consistent, uncertainty is reduced; when it is fragmented, employees tend to rely on informal practices or personal judgement.

This becomes more critical in digital workplaces, where employees operate in decentralised environments and make decisions without direct supervision. In these contexts, communication must provide continuous and context-relevant guidance. Wuersch et al. (2024) and Saeed (2023) show that employee behaviour is shaped by the combined effect of communication, organisational support, and training. When communication is disconnected from workflows, employees are more likely to rely on routines rather than formal guidance.

However, communication does not always produce positive outcomes. Poorly structured or inconsistent communication can create ambiguity and normalise insecure practices. Rice and Searle (2022) show that such conditions may contribute to insider-related risks, highlighting the need for communication to be actively managed and aligned with organisational objectives.

Higher levels of internal communication satisfaction are associated with greater employee engagement (Tkalac Verčič & Pološki Vokić, 2017). More engaged employees are more likely to follow security procedures and report potential issues. Communication therefore

functions not only as an informational tool, but also as a mechanism that supports accountability and consistent behaviour.

Overall, organisational cybersecurity depends not only on the existence of policies or technologies, but on how internal communication enables their consistent interpretation and application in everyday work. It is through these communication processes that security expectations become actionable, shaping whether formal requirements are effectively enacted or informally bypassed in practice.

Discussion: Integrating Behaviour, Culture and Internal Communication in Cybersecurity

Organisational cybersecurity is frequently approached as a technical issue. However, this view fails to explain why security breakdowns persist despite increasing technological investment. While technological controls remain essential, their effectiveness depends on how they are interpreted and applied within organisational settings shaped by human behaviour, information security culture, and internal communication. Rather than reflecting a lack of controls, the problem lies in how these are embedded in practice.

Building on prior research, employees play a dual role in organisational cybersecurity. They can introduce vulnerabilities, for example by falling for phishing attempts, making biased decisions, or not consistently following security policies (Bulgurcu et al., 2010; Shahbaznezhad et al., 2021; Aschwanden et al., 2024). At the same time, they also act as a line of defence. In practice, security-related decisions are embedded in everyday work, where competing priorities and operational constraints influence how controls are applied. These conditions do not simply confirm prior findings but highlight why awareness-based approaches remain structurally limited in practice, thereby challenging the assumption that compliance can be achieved through control mechanisms alone (Alshaikh, 2020).

Security behaviour develops within an organisational context. Shared norms and expectations influence how employees interpret and respond to security requirements (Alhogail, 2015; Da Veiga et al., 2020). However, these expectations do not automatically translate into consistent practice. This disconnect points to a limitation in approaches that treat culture as a stable driver of behaviour, without considering how it is enacted in everyday work. Sustained behavioural alignment depends not only on reinforcement, but on the extent to which security practices are integrated into operational routines. Evidence from phishing reporting studies (Petrič & Just, 2025) further shows that outcomes depend on how deeply these principles are embedded in daily work.

Internal communication connects these elements by translating expectations into actionable guidance and reducing uncertainty in decision-making. Its role goes beyond information transmission, as it shapes how policies are interpreted and enacted in practice (Barlow et al., 2018; Hu et al., 2012). Its effectiveness, however, depends on organisational conditions, particularly leadership. When leaders consistently emphasise security, employees are more likely to recognise its relevance, reinforcing shared expectations and accountability (Men & Stacks, 2014; Goo et al., 2014). Communication, therefore, is not neutral, but actively shapes how security is prioritised in practice.

In practice, a persistent gap often emerges between formal security policies and everyday work. Employees frequently adapt procedures to meet operational demands, for example by bypassing authentication steps or using informal communication channels to meet urgent deadlines. This does not necessarily reflect a lack of awareness, but rather the need to manage trade-offs between security requirements and task efficiency in dynamic work environments (Bulgurcu et al., 2010; Pollini et al., 2022). The gap is not incidental, but structural, reflecting a misalignment between formal security design and operational realities. It also suggests that standardised approaches to cybersecurity awareness may be

inherently limited, as employees differ in how they perceive and respond to cyber risks. As a result, one-size-fits-all interventions are unlikely to be effective across organisational contexts, reinforcing the need for more tailored and behaviourally informed approaches (Aschwanden et al., 2024).

Such dynamics highlight inherent trade-offs between security and usability. When controls are overly rigid or misaligned with operational realities, employees may circumvent them to maintain efficiency. In this context, non-compliance can emerge as a rational and situational response rather than a behavioural failure. This challenges traditional views that interpret non-compliance primarily as a lack of awareness or discipline. As a result, restrictive measures may unintentionally increase risk by encouraging informal workarounds. This reinforces the need to design security practices that align with how work is performed, rather than how it is assumed to occur.

These tensions become more pronounced in digital and hybrid work environments. Distributed teams rely on multiple communication platforms, making consistent security behaviour more difficult to maintain. While informal channels support coordination, they may also bypass formal controls, increasing organisational complexity. Here, flexibility and control should not be seen as opposing forces, but as interdependent elements that must be managed together. Under these conditions, continuous and context-aware communication becomes critical to sustain alignment between expectations and practice.

The analysis is based on existing literature and may not fully capture the complexity of real organisational contexts. Differences across industries, organisational size, and levels of digital maturity may influence how these dynamics unfold in practice. Accordingly, these relationships should be understood as context dependent.

From an organisational perspective, the implications extend beyond implementing improved communication practices, many of which are already recognised in cybersecurity management. The key issue lies in how these practices are conceptualised and used. Cybersecurity should not treat internal communication as a supporting function for awareness or alignment, but as a structural mechanism that determines how security is enacted in practice. In this sense, communication does not simply facilitate compliance; it shapes the conditions under which compliance becomes possible or unworkable. As a result, its role is not to reinforce predefined controls, but to continuously mediate between security requirements and operational realities, influencing whether those controls are followed, adapted, or bypassed.

At its core, the challenge of cybersecurity lies in the misalignment between how security is designed and how work is performed. Addressing this requires moving beyond control-based approaches and recognising security as an organisational capability embedded in everyday practices, where behaviour, internal communication, and operational processes are inherently interconnected.

Conclusion

Organisational cybersecurity cannot be addressed effectively through technological investment alone. Its effectiveness depends on how communication, culture, and employee behaviour interact in everyday work, shaping how security requirements are interpreted and enacted in practice.

These findings indicate that cybersecurity challenges cannot be fully understood within a technical framework, as they are fundamentally shaped by organisational and behavioural dynamics. Employees play a central role in this process, as their day-to-day decisions determine how security is implemented in real contexts. These decisions, however, are influenced by competing operational demands and are not consistently aligned with formal requirements.

Rather than being incidental, the gap between formal security controls and everyday practices reflects a structural misalignment between security design and operational realities. Internal communication plays a critical role in addressing this misalignment by translating expectations into actionable guidance and supporting their application in real work conditions.

These findings have direct organisational implications. Treating cybersecurity as a purely technical function reinforces the disconnect between formal policies and operational practices. Addressing this requires not only technological investment, but also communication practices that are continuous, context-aware, and embedded in everyday workflows.

At the same time, organisations must actively manage the trade-offs between control and flexibility. Overly rigid measures may encourage informal workarounds, while insufficient control may weaken accountability. Managing this tension is therefore central to the effective implementation of cybersecurity practices.

From a practical perspective, organisations need to move beyond isolated training initiatives and adopt communication approaches integrated into everyday work. Security should not be treated as a separate activity, but as part of routine task execution. This requires aligning communication with operational processes and supporting employees in applying security requirements under real conditions.

Ultimately, cybersecurity should be reframed as an organisational process rather than a technical function. Without alignment between behaviour, culture, and communication in everyday work, technological solutions alone are unlikely to deliver effective or sustainable outcomes.

Declaration of the use of IA

During the preparation of this article, the author used AI-based tools, including Gemini, Grammarly and Deepl, to support text structuring, improve clarity, and refine academic language. All outputs generated by these tools were critically reviewed, validated, and adapted by the author. The author takes full responsibility for the content, ensuring its accuracy, originality, and compliance with ethical and academic standards.

References

Alhogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior, 49, 567–575*. https://doi.org/10.1016/j.chb.2015.03.054

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behaviour: A practice perspective. *Computers & Security, 98, 102003.* https://doi.org/10.1016/j.cose.2020.102003

Aschwanden, R., Messner, C., Höchli, B., & Holenweger, G. (2024). Employee behaviour: The psychological gateway for cyberattacks*. Organisational Cybersecurity Journal: Practice, Process & People, 4*(1), 32–50. https://doi.org/10.1108/OCJ-02-2023-0004

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. (2018). Don't even think about it! The effects of antineutralization, informational, and normative communication on information security compliance. Journal of the Association for Information Systems, 19(8),735–777. https://aisel.aisnet.org/jais/vol19/iss8/3/

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–548. https://doi.org/10.2307/25750690

Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security, 49, 162–176*. https://doi.org/10.1016/j.cose.2014.12.006

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security, 92, 101713.* https://doi.org/10.1016/j.cose.2020.101713

Goo, J., Yim, M. S., & Kim, D. J. (2014). A path to successful management of employee security compliance: An empirical study of information security climate. *IEEE Transactions on Professional Communication, 57*(4), 286–308. https://doi.org/10.1109/TPC.2014.2374011

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences, 43*(4), 615–660. https://doi.org/10.1111/j.1540-5915.2012.00361.x

Men, L. R., & Stacks, D. W. (2014). The effects of authentic leadership on strategic internal communication and employee–organization relationships. *Journal of Public Relations Research, 26*(4), 301–324. https://doi.org/10.1080/1062726X.2014.908720

Petrič, G., & Just, J. N. (2025). Information security culture and phishing-reporting model: Structural equivalence across Germany, UK, and USA. *Journal of Cybersecurity, 11(1), tyaf011.* https://doi.org/10.1093/cybsec/tyaf011

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition, Technology & Work, 24*(2), 371–390. https://doi.org/10.1007/s10111-021-00683-y

Rice, C., & Searle, R. H. (2022). The enabling role of internal organisational communication in insider threat activity: Evidence from a high-security organization. *Management Communication Quarterly, 36(*3), 467–495. https://doi.org/10.1177/08933189211062250

Saeed, S. (2023). Digital workplaces and information security behaviour of business employees: An empirical study of Saudi Arabia. *Sustainability, 15*(7), 6019. https://doi.org/10.3390/su15076019

Shahbaznezhad, H., Kolini, F., & Rashidirad, M. (2021). Employees' behaviour in phishing attacks: What individual, organisational, and technological factors matter? Journal of *Computer Information Systems, 61*(6), 539–550. https://doi.org/10.1080/08874417.2020.1812134

Tkalac Verčič, A., Galić, Z., & Žnidar, K. (2023). The relationship of internal communication satisfaction with employee engagement and employer attractiveness: Testing the joint mediating effect of social exchange quality indicators*. International Journal of Business Communication, 60*(4), 1313–1340. https://doi.org/10.1177/23294884211053839

Vodafone. (2023). *Cyber security factsheet*. Vodafone Group. https://reports.investors.vodafone.com/view/919554535/9/

Wuersch, L., Neher, A., Maley, J. F., & Peter, M. K. (2024). Using a digital internal communication strategy for digital capability development*. International Journal of Strategic Communication, 18*(3), 167–188. https://doi.org/10.1080/1553118X.2024.2330405